Ridgeline Service Advisor Release Note

Software Version 2.0

Extreme Networks, Inc.
3585 Monroe Street
Santa Clara, California 95051
(888) 257-3000
(408) 579-2800
http://www.extremenetworks.com

Part number: 120579-00 Rev. 03

AccessAdapt, Alpine, Altitude, BlackDiamond, EPICenter, ExtremeWorks Essentials, Ethernet Everywhere, Extreme Enabled, Extreme Ethernet Everywhere, Extreme Networks, Extreme Standby Router Protocol, Extreme Turbodrive, Extreme Velocity, ExtremeWare, ExtremeWorks, ExtremeXOS, Go Purple Extreme Solution, ExtremeXOS ScreenPlay, ReachNXT, Ridgeline, Sentriant, ServiceWatch, Summit, SummitStack, Triumph, Unified Access Architecture, Unified Access RF Manager, UniStack, the Extreme Networks logo, the Alpine logo, the BlackDiamond logo, the Extreme Turbodrive logo, the Summit logos, and the Powered by ExtremeXOS logo are trademarks or registered trademarks of Extreme Networks, Inc. or its subsidiaries in the United States and/or other countries.

sFlow is a registered trademark of InMon Corporation.

Specifications are subject to change without notice.

All other registered trademarks, trademarks, and service marks are property of their respective owners.

© 2010 Extreme Networks, Inc. All Rights Reserved.

Contents

Chapter 1: Overview 3

New Hardware Supported in Ridgeline SA 2.0 3
Key Features in Ridgeline SA 2.0 3
Important Information about Using Ridgeline SA 5
About Downloading Software Images from Extreme 5
Determining Device Serial Numbers 6
Providing Serial Numbers to Extreme Networks eSupport 8
The Ridgeline SA RADIUS Server 10
The Ridgeline SA TFTP Server 11
Telnet Polling and Ridgeline SA 11
Ridgeline SA Server Requirements 11
Microsoft Windows 11
Sun Microsystems Solaris 10 12
Red Hat Enterprise Linux Version 5 12
Allowing Clients Access to the Server from Behind a Firewall 13
Ridgeline SA Client Requirements 13
Microsoft Windows 14
Sun Solaris 14
Red Hat Enterprise Linux 14
The Client 14
Modifying the Amount of Memory Available for Java Applets 15
ExtremeWare/ExtremeXOS Support Requirements 15
Switch Access Requirements 16
Ridgeline SA 2.0 Device Support 17
Extreme Networks Device Support 17
Avaya Device Support 18
Other Third-Party Device Support 18
SSH Support 19
Ridgeline SA Software Licensing 19
Software Installation or Upgrade Overview 20
Obtaining a License 20
Ridgeline SA Software Documentation 20

Chapter 2: Clarifications, Known Behaviors, and Resolved Issues 23

Troubleshooting 23
The Package Ridgeline SA Info command 23
Client Information from the About window 23
ExtremeXOS 12.4.2 Dependencies 23
Clarifications and Known Problems 24
Installing or Uninstalling 25
Cannot re-install Ridgeline SA after an unsuccessful uninstall 25
Installing Ridgeline SA on a system with non-English-language character sets 26
General—Client 26
Auto-save is on by default when the Ridgeline SA server starts up 26

Message about Ridgeline SA's digital signature appears twice 26
Multibyte-encoded characters display incorrectly in Ridgeline SA Client 27
Connection error when Ridgeline SA server and client are in different domains....27
General—Server 27
TFTP port remains in use after Ridgeline SA TFTP server disabled 27
Traps may be dropped if the trap rate becomes excessive....27
Stopping the Ridgeline SA database prior to stopping the server 27
Network Views 27
Incorrect display of load-shared links 27
Error when disabling EAPS primary port if EAPS ring was displayed in the Map View 28
Updated EAPS information not displayed in the Table View....28
Invalid Session message displayed when saving a map....28
Alarm Manager 28
HTTP unreachable alarms not generated for certain devices 28
Incorrect Power Supply Failed alarm generated for SNMP-unreachable devices 28
CPU Utilization threshold comes back after being deleted 28
Configuration Manager....28
Downloading a config file to device fails if using SSH 28
Changing the Diff or Config file viewer settings does not work properly 29
Refreshing the Configuration Manager window after a Schedule Baseline operation 29
Device/Port Grouping....29
Cannot have identically named Device and Port groups at the same level....29
Error when creating a new group while deleting another group 29
Error when moving devices to a large group....29
Java error when copying a top-level group to another top-level group 29
Stacking devices may not be displayed in the Hardware Selection page 29
Inventory Management....30
Modify Device changed fields are not updated after Apply 30
Additional Information field accepts more than 255 characters 30
The Upload Device Info command does not work with SSH 30
The ExtremeXOS config file saved by the Upload Device Info command has errors....30
BD8810 port containing a 100Base-FX mini-GBIC displayed as a UTP port....30
IP/MAC Address Finder....30
Ridgeline SA does not use VRs when pinging, resulting in errors on some ExtremeXOS devices. 30
Real-Time Statistics 30
Hierarchical port groups are not displayed correctly in the RT Statistics applet....30
Reports 31
User Defined Reports link does not appear the first time Reports are invoked....31
Internal power supplies reported as failed rather than powered off on Summit X250 or X450 devices 31
Telnet 31
Cannot edit ExtremeXOS Policy files in the Telnet window....31
VLAN Management....31
Cannot create a VLAN Network Name with the same name as a device/port group 31
Enabling "Show VLANs" in the Link Details window displayed incorrect information....31
Avaya-Ridgeline SA Integration....32
Ridgeline SA complains about missing device when launched from AIM 32
Attempting to launch Ridgeline SA from the browser-based AIM Console fails....32
Profile Manager....32
Ridgeline SA does not enforce the maximum number of profiles 32
Profiles bound to USER-REQUEST events are executed at the time of deployment 32
Scripting 32
Error when trying to save a Ridgeline SA script....32

1 Overview

This release note contains a summary of the requirements and new features for the Ridgeline Service Advisor™ Management Suite, version 2.0.

- See "New Hardware Supported in Ridgeline SA 2.0" for a list of the new Extreme Networks devices supported in this release.
- See Table 3 for a full list of the Extreme Networks devices supported by Ridgeline SA 2.0.

Please refer to the *Ridgeline Service Advisor Reference Guide* for detailed descriptions of the features in the Ridgeline SA 2.0 release.

Contact customer support at (408) 579-2800 or support@extremenetworks.com if you need additional help.

This section covers the following topics:

- New Hardware Supported in Ridgeline SA 2.0 on page 3
- Key Features in Ridgeline SA 2.0 on page 3
- About Downloading Software Images from Extreme on page 5
- Ridgeline SA Server Requirements on page 11
- Ridgeline SA Client Requirements on page 13
- ExtremeWare/ExtremeXOS Support Requirements on page 15
- Ridgeline SA 2.0 Device Support on page 17
- Software Installation or Upgrade Overview on page 20
- Obtaining a License on page 20
- Ridgeline SA Software Documentation on page 20

New Hardware Supported in Ridgeline SA 2.0

The following Extreme Networks devices are supported in Ridgeline SA 2.0:

- Summit X480 series switches
- BlackDiamond 20804 switch
- 8500-MSM24 module
- 8500-G48T-e module
- 8500-G24X-e module

Key Features in Ridgeline SA 2.0

- **New platform support.** You can now install the Ridgeline SA server on the Windows 2008 Server platform. In addition, Ridgeline SA now supports both the 32-bit and 64-bit versions of supported

Windows platforms, as well as the 32-bit and 64-bit versions of the supported Red Hat Enterprise Linux platform.

- **Map view of all devices in your network.** The new All Map option under Network Views displays a graphical view of all of the devices managed by Ridgeline SA. From the All Map view, you can see a map view, navigation table, and details panel containing information about all the managed devices in your network.
- **Customizable Ridgeline SA Home Page.** You can select which reports populate the Ridgeline SA Home Page, allowing you to display a convenient, dashboard-like view of data relevant to your network.
- **Point-and-click network provisioning.** Ridgeline SA's new provisioning features simplify network configuration tasks with selectable options in dialog boxes. Ridgeline SA automatically validates the options you've selected prior to deploying the configuration to managed devices, ensuring that the configuration is correct before it goes into production.
- **VLAN and VMAN (PB/Q-in-Q) provisioning.** Using the Ridgeline SA provisioning interface, you can create a VLAN or VMAN simply by selecting the devices, ports, and tagging options you want, then validate and deploy the VLAN or VMAN configuration with a single mouse click.

  VLAN provisioning is supported on Extreme switches running ExtremeXOS 11.6 and higher, and ExtremeWare 7.7 and higher. VMAN provisioning is supported on Extreme switches running ExtremeXOS 12.1 and higher.
- **Job Scheduler.** You can use the new Job Scheduler feature to execute Ridgeline SA functions on specified devices at specified times. Ridgeline SA scripts can now be configured as *script tasks*, which can run automatically at designated times.
- **VPLS discovery and visualization.** With the Advanced Services Pack, Ridgeline SA can discover the Virtual Private LAN Service (VPLS) configuration on the managed devices in your network, and display an overlay view of selected VPLS instances, including information about specific pseudo wires. Ridgeline SA scripts can create VPLS instances and configure devices as VPLS peers.

  VPLS is supported on Extreme switches running ExtremeXOS 12.4 and higher.
- **PBB discovery, visualization, and provisioning.** With the Advanced Services Pack, Ridgeline SA identifies the Service VLANs (SVLANs), Backbone VLANs (BVLANs), Customer VLANs (CVLANs), and Extended Service ID (ISID) instances in your Provider Backbone Bridge (PBB) networks. You can display an overlay view of a selected PBB network, along with detailed information about PBB components in Ridgeline SA tables. Ridgeline SA's PBB provisioning feature allows you to create BVLANs on selected devices, ports, or links, as well as modify and delete existing BVLANs.

  PBB is supported on BlackDiamond 20800 series switches running ExtremeXOS 12.4 and higher.
- **Ethernet service provisioning.** Using the service provisioning wizard, you can create E-Line (point-to-point) and E-LAN (multipoint-to-multipoint) services. You can select the devices and ports that make up the service, specify the transport method (VLAN, VMAN, or PBB), create and apply bandwidth profiles, then validate the configuration and deploy it on your network.

  The Services view provides at-a-glance information about Ethernet services, the devices and ports where they are configured, and details about the transport method specified for each service.

  Device support for E-Line and E-LAN services depends on the transport method used with the service:

  - VLAN: ExtremeXOS 11.6 and higher; ExtremeWare 7.7 and higher.
  - VMAN: ExtremeXOS 12.1 and higher.
  - PBB: ExtremeXOS 12.4 and higher.

- **EAPS provisioning.** You can use the EAPS provisioning feature to configure new EAPS domains, including specifying member links, the EAPS master node, primary and secondary ports, control VLAN, hello timer, and fail timer parameters. Your configuration is validated by the software before it is deployed to managed devices.

  EAPS provisioning is supported on Extreme switches running ExtremeXOS 12.4 and higher.

Important Information about Using Ridgeline SA

The following describes some important caveats about how Ridgeline SA should be used within your network.

About Downloading Software Images from Extreme

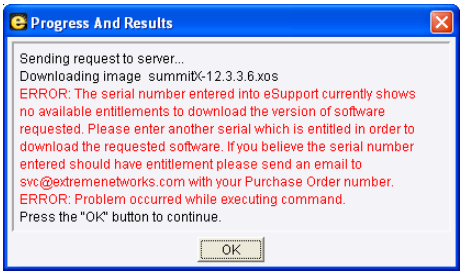
Using the Ridgeline SA Firmware Manager, you can download software and BootROM images from Extreme Networks to your Ridgeline SA server, then upgrade the devices in your network with the new images. In order to download the new images from Extreme, you must have a current support contract and an Extreme Networks eSupport user name and password.

You also need to provide eSupport with the serial number of a device of the type you are upgrading in order to obtain updated images for that type of device. For example, to obtain updated Summit X650 software, you need to provide the serial number of one of the Summit X650 switches in your network prior to downloading the software. After you do this, the updated Summit X650 software can be downloaded from Extreme, and you can use it to upgrade any of the Summit X650 switches in your network. For chassis devices, you provide the serial number of a Management Module or I/O Module.

Once you have provided the serial number for the device, you can download subsequent image updates for that type of device without having to enter the serial number again.

If you have not yet provided eSupport with a serial number for the device type you are upgrading, you may see the following window when you attempt to download a new image using Firmware Manager:

Figure 1: Progress and Results window showing unsuccessful image download

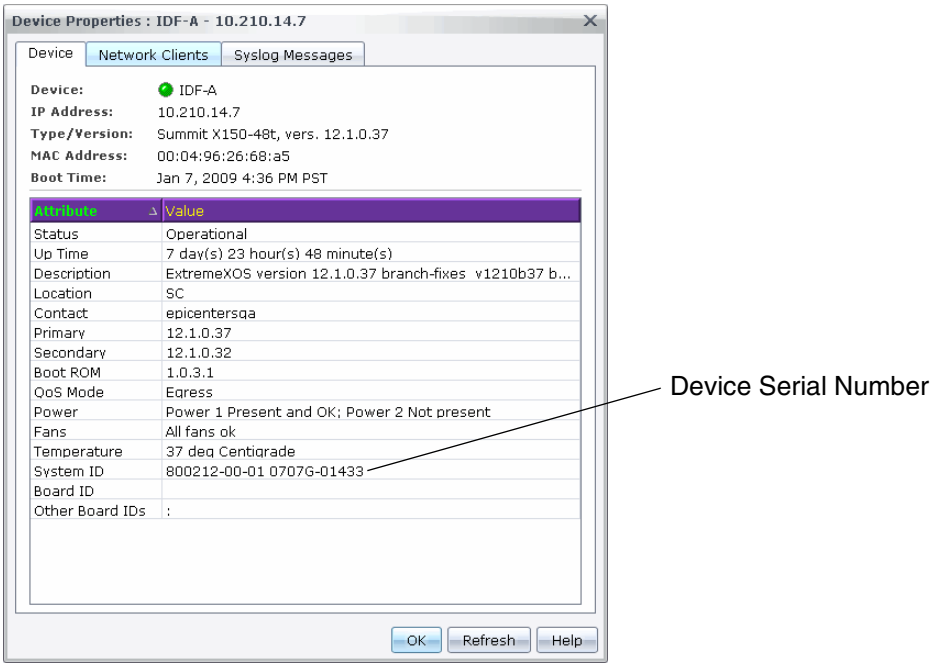

Progress And Results
Sending request to server...
Downloading image summitX-12.3.3.6.xos
ERROR: The serial number entered into eSupport currently shows no available entitlements to download the version of software requested. Please enter another serial which is entitled in order to download the requested software. If you believe the serial number entered should have entitlement please send an email to svc@extremenetworks.com with your Purchase Order number.
ERROR: Problem occurred while executing command.
Press the "OK" button to continue.
OK

To obtain the new images, you must determine the serial numbers for the types of device that you want to upgrade, then supply those serial numbers to Extreme Networks eSupport. After you do this, the software images download normally.

Determining Device Serial Numbers

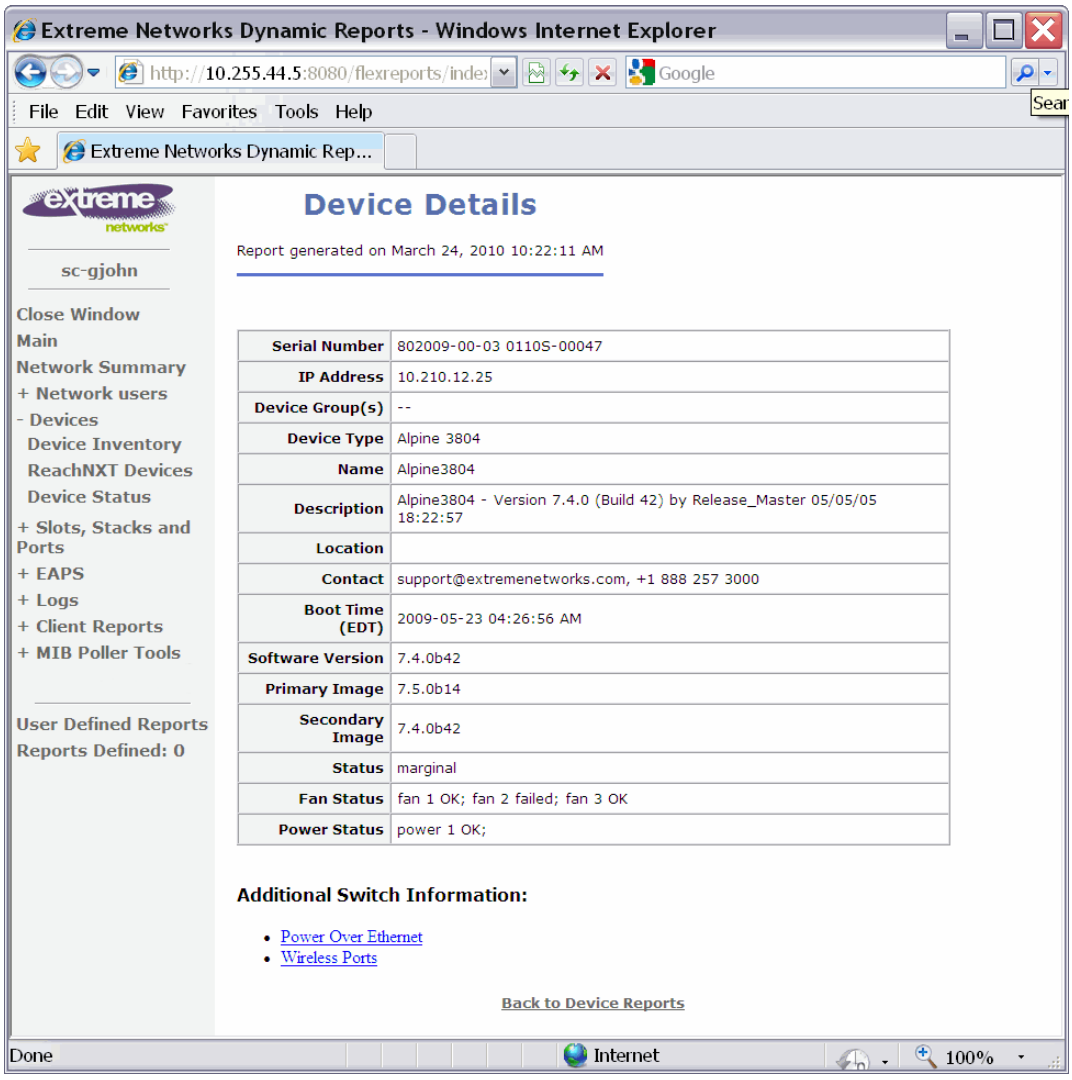
The serial number for a device is displayed in the Device Properties window. To display this window, select a device, then select **Properties** from the **File** menu, or from the right-click pop-up menu. The device serial number appears in the System ID field, as shown in Figure 2.

Figure 2: Location of Serial Number in the Device Properties window



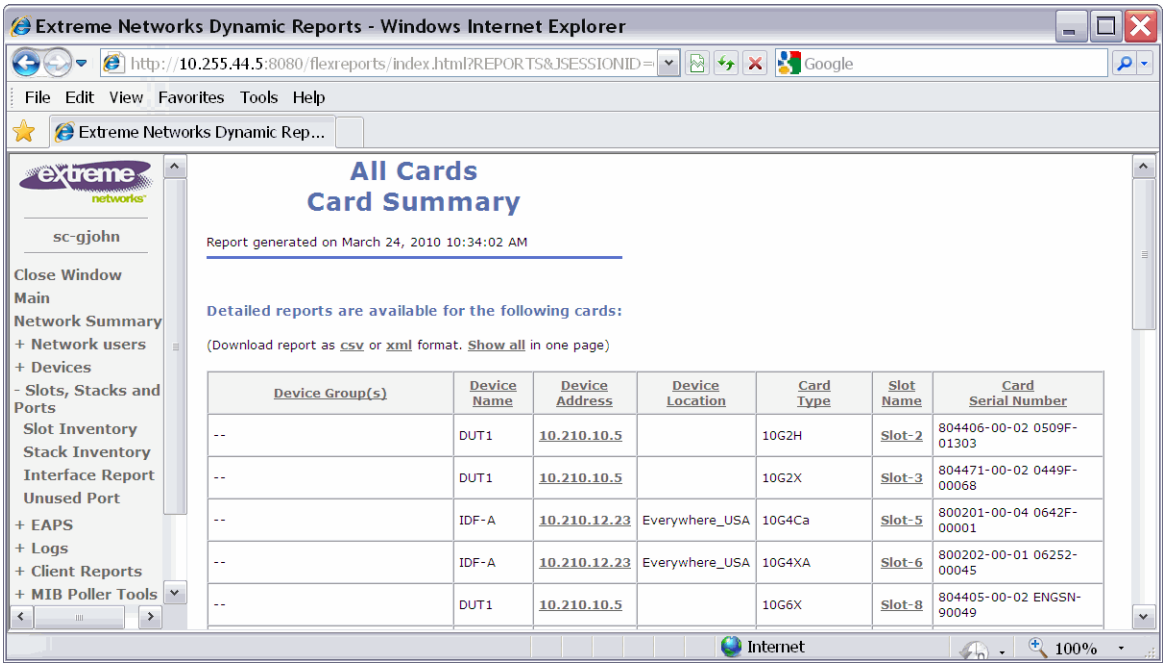
You can also display the serial numbers of devices in your network by running a Device Details report in Ridgeline SA. For example:

Figure 3: Device Details Report



To display the serial numbers of individual modules, run the Card Summary report. For example:

Figure 4: All Cards Card Summary Report

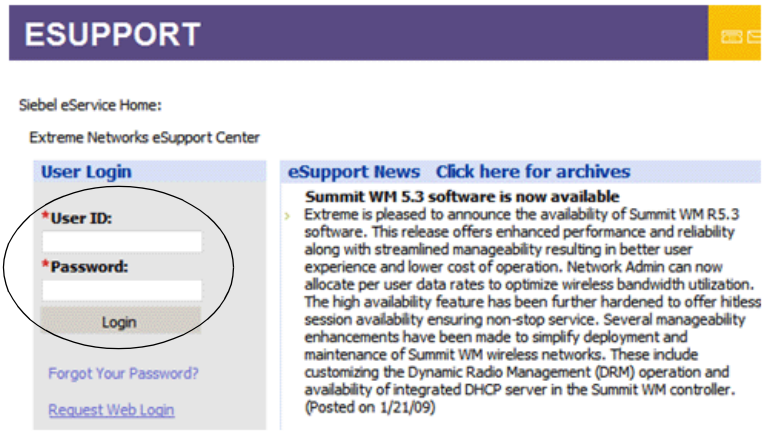

Extreme Networks Dynamic Reports - Windows Internet Explorer
http://10.255.44.5:8080/flexreports/index.html?REPORTS&JSESSIONID=
File Edit View Favorites Tools Help
Extreme Networks Dynamic Rep...
sc-gjohn
Close Window
Main
Network Summary
+ Network users
+ Devices
- Slots, Stacks and Ports
Slot Inventory
Stack Inventory
Interface Report
Unused Port
+ EAPS
+ Logs
+ Client Reports
+ MIB Poller Tools
All Cards
Card Summary
Report generated on March 24, 2010 10:34:02 AM
Detailed reports are available for the following cards:
(Download report as csv or xml format. Show all in one page)
Device Group(s) | Device Name | Device Address | Device Location | Card Type | Slot Name | Card Serial Number
-- | DUT1 | 10.210.10.5 | | 10G2H | Slot-2 | 804406-00-02 0509F-01303
-- | DUT1 | 10.210.10.5 | | 10G2X | Slot-3 | 804471-00-02 0449F-00068
-- | IDF-A | 10.210.12.23 | Everywhere_USA | 10G4Ca | Slot-5 | 800201-00-04 0642F-00001
-- | IDF-A | 10.210.12.23 | Everywhere_USA | 10G4XA | Slot-6 | 800202-00-01 06252-00045
-- | DUT1 | 10.210.10.5 | | 10G6X | Slot-8 | 804405-00-02 ENGSN-90049
Internet
100%

Providing Serial Numbers to Extreme Networks eSupport

To provide serial numbers to Extreme Networks eSupport, do the following:

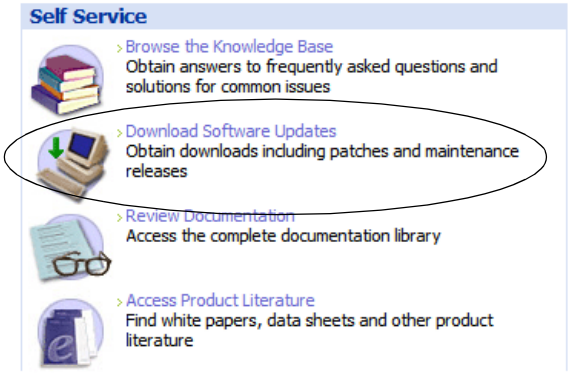
1 Go to www.extremenetworks.com and log into the eSupport page with your eSupport user ID and password.

Figure 5: eSupport Login page


ESUPPORT
Siebel eService Home:
Extreme Networks eSupport Center
User Login
*User ID:
*Password:
Login
Forgot Your Password?
Request Web Login
eSupport News Click here for archives
Summit WM 5.3 software is now available
Extreme is pleased to announce the availability of Summit WM R5.3 software. This release offers enhanced performance and reliability along with streamlined manageability resulting in better user experience and lower cost of operation. Network Admin can now allocate per user data rates to optimize wireless bandwidth utilization. The high availability feature has been further hardened to offer hitless session availability ensuring non-stop service. Several manageability enhancements have been made to simplify deployment and maintenance of Summit WM wireless networks. These include customizing the Dynamic Radio Management (DRM) operation and availability of integrated DHCP server in the Summit WM controller.
(Posted on 1/21/09)

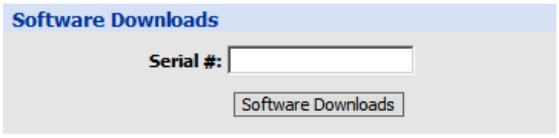
2 Select the **Download Software Updates** link.

Figure 6: Download Software Updates link on eSupport page


Self Service
Browse the Knowledge Base
Obtain answers to frequently asked questions and solutions for common issues
Download Software Updates
Obtain downloads including patches and maintenance releases
Review Documentation
Access the complete documentation library
Access Product Literature
Find white papers, data sheets and other product literature

3 In the Serial # box, enter the serial number of the device or module, and click **Software Downloads**.

Figure 7: Serial number entry box

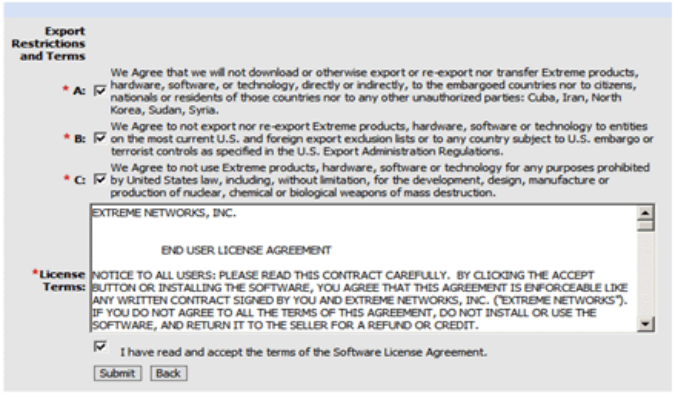


NOTE

For chassis devices, you must provide the serial number of a Management Module or I/O Module.

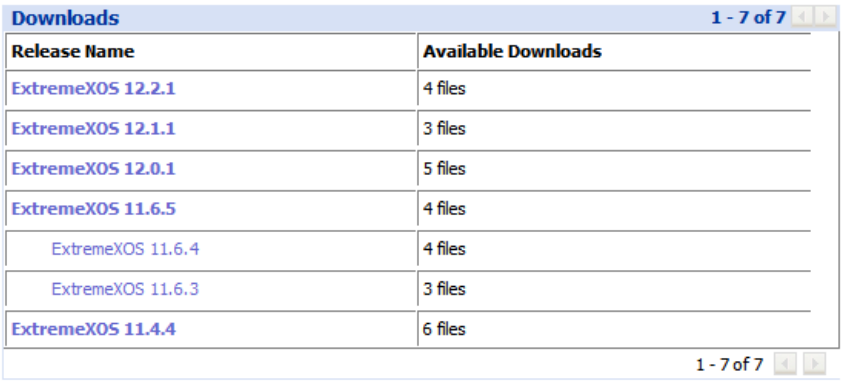
4 Accept the terms of the software license agreement and click **Submit**.

Figure 8: Software license agreement


Export Restrictions and Terms
* A: We Agree that we will not download or otherwise export or re-export nor transfer Extreme products, hardware, software, or technology, directly or indirectly, to the embargoed countries nor to citizens, nationals or residents of those countries nor to any other unauthorized parties: Cuba, Iran, North Korea, Sudan, Syria.
* B: We Agree to not export nor re-export Extreme products, hardware, software or technology to entities on the most current U.S. and foreign export exclusion lists or to any country subject to U.S. embargo or terrorist controls as specified in the U.S. Export Administration Regulations.
* C: We Agree to not use Extreme products, hardware, software or technology for any purposes prohibited by United States law, including, without limitation, for the development, design, manufacture or production of nuclear, chemical or biological weapons of mass destruction.
*License Terms:
EXTREME NETWORKS, INC.
END USER LICENSE AGREEMENT
NOTICE TO ALL USERS: PLEASE READ THIS CONTRACT CAREFULLY. BY CLICKING THE ACCEPT BUTTON OR INSTALLING THE SOFTWARE, YOU AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN CONTRACT SIGNED BY YOU AND EXTREME NETWORKS, INC. ("EXTREME NETWORKS"). IF YOU DO NOT AGREE TO ALL THE TERMS OF THIS AGREEMENT, DO NOT INSTALL OR USE THE SOFTWARE, AND RETURN IT TO THE SELLER FOR A REFUND OR CREDIT.
I have read and accept the terms of the Software License Agreement.
Submit
Back

A table of the software versions available for the device is displayed. If the device is under a service contract, all software versions are displayed; otherwise, only software versions available for the 90-day warranty period are displayed. For example:

Figure 9: List of available software versions for a device



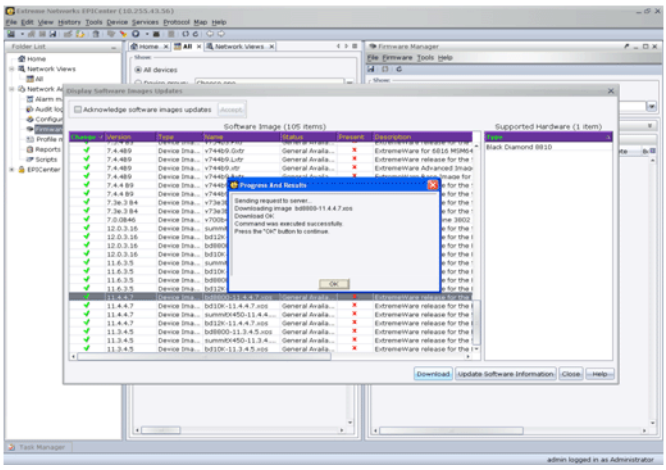
Downloads 1 - 7 of 7

Release Name	Available Downloads
ExtremeXOS 12.2.1	4 files
ExtremeXOS 12.1.1	3 files
ExtremeXOS 12.0.1	5 files
ExtremeXOS 11.6.5	4 files
ExtremeXOS 11.6.4	4 files
ExtremeXOS 11.6.3	3 files
ExtremeXOS 11.4.4	6 files

1 - 7 of 7

5 In the Ridgeline SA Firmware Manager, select one of the software versions listed in the eSupport table. When you do this, the software image is downloaded to the Ridgeline SA server.

Figure 10: Downloading a selected software image to the Ridgeline SA server



The Ridgeline SA RADIUS Server

Ridgeline SA's built-in RADIUS server should not be used to provide authentication services for your network devices in a production environment. It should be used only for demonstration or testing purposes. The built-in server is not sufficiently robust to be used in a production environment. For RADIUS authentication, Ridgeline SA can be configured to function as a client of an external RADIUS authentication server.

The Ridgeline SA TFTP Server

Ridgeline SA's built-in TFTP server is intended only for uploading and downloading switch configuration files and software image files under Ridgeline SA's control. It is not intended for use as a general purpose TFTP server.

Telnet Polling and Ridgeline SA

Although Ridgeline SA primarily uses SNMP to retrieve switch status and configuration information, it uses Telnet polling to collect certain types of information that are not available using SNMP. This includes information about netlogins, device FDB data (if FDB polling is enabled) and other selected status. Ridgeline SA's use of Telnet polling can affect your switches in several ways:

- Each time Ridgeline SA logs in and out of the switch, entries are created in the switch log.
- In some cases Ridgeline SA needs to disable CLI paging in order to parse the results of certain commands. This creates an entry into the switch log file each time this occurs.
- Over time, these entries can fill the switch log file, and can make it more difficult to recognize log entries due to errors or other significant conditions. If these entries in the log file become problematic, there are several possible steps you can take to alleviate the problem, including periodically clearing the switch log, disabling Ridgeline SA's Telnet polling, reducing Ridgeline SA's polling frequency, or using the ExtremeWare or ExtremeXOS Event Management System log filtering capability to suppress the log entries generated by Ridgeline SA login and logout events.

Ridgeline SA Server Requirements

The Ridgeline SA 2.0 server is supported on Windows Vista, XP, 2003 Server or 2008 Server, on SPARC workstations running Solaris 10, or on systems running Red Hat Enterprise Linux version 5.

Specific details as to versions supported, as well as hardware and software requirements, are described in the following subsections.

NOTE

Prior to installing Ridgeline SA, make sure the system where you are installing the software is DNS-resolvable and accessible both by IP address and by hostname from all machines where the Ridgeline SA client will be launched. If it is not, add an entry for the system in the local DNS server or the hosts file on the client machines.

Microsoft Windows

The system requirements for the Ridgeline SA server under Microsoft Windows are as follows:

- Microsoft Windows Vista, Windows XP Professional with SP1 or later, Windows 2003 Server, or Windows 2008 Server running on an Intel Pentium-compatible CPU.

  Both 32-bit and 64-bit versions of the Windows operating system are supported.
- 2 GB RAM minimum, 4 GB recommended.

  Up to 4 GB may be needed for very large numbers of devices (1000 or more).
- 2 GB disk space available, NTFS filesystem recommended.

- Swap space equal to double the amount of memory. For example, if you have 512 MB of RAM, you should have 1 GB of swap space.
- 1 GHz or greater Pentium-compatible processor (2 GHz recommended).

The Ridgeline SA server software requires the 1.6.0_10 (or higher) Java runtime package. The 1.6.0_10 Java runtime package is included in the server installation, and that is the version we recommend you use.

NOTE

Additional disk space may be needed to hold alarm logs and other runtime data. The amount of space depends on the number of devices and the number of traps and syslog messages generated by the managed devices.

Sun Microsystems Solaris 10

The Ridgeline SA server software, version 2.0, is supported under the Sun Solaris Operating Environment, version 10 (64-bit version) on SPARC systems. The system requirements for the server are as follows:

- 2 GB RAM minimum, 4 GB recommended.

  Up to 4 GB may be needed for very large numbers of devices (1000 or more).
- 400 Mhz or better processor.
- 2 GB disk space available.
- Swap space equal to double the amount of memory. For example, if you have 512 MB of RAM, you should have 1 GB of swap space.

The Ridgeline SA server software requires the 1.6.0_10 (or higher) Java runtime package. The 1.6.0_10 Java runtime package is included in the server installation, and that is the version we recommend you use.

Please make sure you have the most current OS patch downloads installed before you run the Ridgeline SA server in a Solaris environment. To obtain the latest patches for the version of Solaris you are running, visit:
http://sunsolve.sun.com/show.do?target=patches/JavaSE

NOTE

Additional disk space may be needed to hold alarm logs and other runtime data. The amount of space depends on the number of devices and the number of traps and syslog messages generated by the managed devices.

Red Hat Enterprise Linux Version 5

The Ridgeline SA server software, version 2.0, is supported under Red Hat Enterprise Linux version 5. Both 32-bit and 64-bit versions of the operating system are supported, only on x86-based platforms. The system requirements are as follows:

- 2 GB RAM minimum, 4 GB recommended.

  Up to 4 GB may be needed for very large numbers of devices (1000 or more).
- 1 GHz or greater Pentium-compatible processor (2 GHz recommended).

- 2 GB disk space available.
- Swap space equal to double the amount of memory. For example, if you have 512 MB of RAM, you should have 1 GB of swap space.
- A GUI/Desktop environment must be installed on the server machine.

The Ridgeline SA server software requires the 1.6.0_10 (or higher) Java runtime package. The 1.6.0_10 Java runtime package is included in the server installation, and that is the version we recommend you use.

NOTE

Additional disk space may be needed to hold alarm logs and other runtime data. The amount of space depends on the number of devices and the number of traps and syslog messages generated by the managed devices.

Allowing Clients Access to the Server from Behind a Firewall

If the Ridgeline SA server is located behind a firewall, you must allow Ridgeline SA clients access through the firewall. To do this, use the following procedure:

1. Launch the Ridgeline SA client from the same machine were the server is installed.
2. Expand the Ridgeline SA Administration folder
3. Click Users, Roles & Servers
4. Click the Server Properties tab
5. Select Other from the drop-down list
6. In the Client Port field, specify an available port number (the default of 0 means any random available port)
7. Click **Apply** to apply the setting.
8. Stop and restart the Ridgeline SA server. For instructions, see the Ridgeline SA Installation and Upgrade Guide.
9. In the settings for your firewall, allow exceptions for the following ports:
   - The HTTP port used for communication with Ridgeline SA clients (default is 8080)
   - Port 3873
   - The Client Port you specified in step 6 above

Ridgeline SA Client Requirements

A Ridgeline SA client requires a monitor that supports 1024 x 768 resolution, and at least 16-bit color. Your system display settings must be set for at least 65536 colors.

The client can use large amounts of memory. 256 MB of RAM is the minimum for best performance. An additional 512 MB is required if you plan to launch the client from the same system as the Ridgeline SA server.

Microsoft Windows

The system requirements for the Ridgeline SA client under Microsoft Windows are as follows:

- Windows Vista, XP Professional with SP1 or later, Windows 2003 Server, or Windows 2008 Server running on an Intel Pentium-compatible CPU.
- A monitor that supports at least 1024 x 768 resolution, and 16-bit color. Your system display settings must be set for at least 65536 colors.
- 512 MB RAM minimum (1 GB recommended).
- A browser is required to log on to Ridgeline SA, display reports, and view the Ridgeline SA on-line Help.

Sun Solaris

The system requirements for the Ridgeline SA client under Solaris are as follows:

- SPARC workstation
- A monitor that supports at least 1024 x 768 resolution, and 16-bit color. Your system display settings must be set for at least 65536 colors.
- 512 MB RAM minimum.
- A browser is required to log on to Ridgeline SA, display reports, and view the Ridgeline SA on-line Help.

Red Hat Enterprise Linux

The system requirements for the Ridgeline SA client under Red Hat Enterprise Linux version 5 are as follows:

- A monitor that supports at least 1024 x 768 resolution, and 16-bit color. Your system display settings must be set for at least 65536 colors.
- 512 MB RAM minimum (1 GB recommended).
- A browser is required to log on to Ridgeline SA, display reports, and view the Ridgeline SA on-line Help.

The Client

The Ridgeline SA client can be launched by logging on to the server from a browser. Ridgeline SA uses signed applets: you will be prompted to accept the security certificate from Extreme Networks the first time you try to launch the applet.

NOTE

The Java Plug-In version 1.6.0_10 (or higher) is required by the Ridgeline SA client. If the minimum required version of the plug-in is not already installed, you will be prompted to download it the first time you try to launch the Ridgeline SA client.

Table 1 lists the browsers that are supported by the Ridgeline SA 2.0 release. A browser is also required to display Ridgeline SA reports and the Ridgeline SA on-line Help.

Table 1: Ridgeline SA 2.0 Supported Browsers

Platform	Minimum Browser Configuration
Microsoft Windows	Internet Explorer™ 6.0, 7.0, 8.0; Mozilla Firefox 1.5, 2.0, 3.0
Sun Solaris 10	Mozilla Firefox 1.5, 2.0, 3.0
Red Hat Enterprise Linux 5	Mozilla Firefox 3.0

NOTE

For the Mozilla Firefox browser, you must install the Java Plug-In, then link the plug-in to the Firefox browser. See the Ridgeline SA Installation and Upgrade Guide *for instructions.*

Modifying the Amount of Memory Available for Java Applets

By default, Java applets can consume only up to 64MB of memory. This may not be enough to allow Ridgeline SA to function effectively. Java applets without sufficient memory may start up and run very slowly, or may generate an Out of Memory error. You can increase the amount of memory available to applets through the Java Plug-in control Panel. The following instructions apply to JRE 1.6.0.

To increase the memory available to Java applets, do the following:

1 Go to the Windows Control Panel.

2 Click the Java icon to launch the Java Control Panel.

3 Click the Java tab

4 Under Java Applet Runtime Settings, click the **View...** button.

5 Double-click the field labeled Java Runtime Parameters, type the following line exactly as shown, then click **OK**.

```
-Xmx256M
```

6 Click **Apply**. Restart the browser to have these settings take effect.

ExtremeWare/ExtremeXOS Support Requirements

Table 2 describes the minimum ExtremeWare or ExtremeXOS software image versions for each switch platform supported in Ridgeline SA release 2.0. Make sure that you have these software images or later versions running on your Extreme switches before running Ridgeline SA.

Table 2: ExtremeWare/ExtremeXOS Versions Supported by Ridgeline SA 2.0

Extreme Switch Platform	ExtremeWare Versions Supported
Summit 150	ExtremeXOS 12.0 SR1 or later
Summit 200	7.1e or later (*Note:* S200s stacking not supported in 7.1e. Please upgrade to 7.4 for stacking support). 7.3e or later required for 802.1x and SNMPv3 support 7.4 or later required for S200s stacking support.
Summit 300-24	7.3e or later

Table 2: ExtremeWare/ExtremeXOS Versions Supported by Ridgeline SA 2.0 (continued)

Extreme Switch Platform	ExtremeWare Versions Supported
Summit 300-48	6.2a or later 7.3e or later required for 802.1x and SNMPv3 support
Summit 400-24	7.4 or later
Summit 400-48	7.2e or later 7.3e or later required for 802.1x and SNMPv3 support 7.4 or later required for S400s stacking support.
All *"i"* Series switches, Alpine, MSM64*i*	6.2 or later 7.1 or later required for 802.1x and SNMPv3 support
Summit X250	ExtremeXOS 12.0 or later
Summit X250e	ExtremeXOS 12.0 or later
	ExtremeXOS 12.0 SR1 or later for X250e-24x
Summit X350	ExtremeXOS 12.0 or later
Summit X450	ExtremeXOS 11.2 or later
	ExtremeXOS 11.5 or later for X450e, X450a
Summit X480	ExtremeXOS 12.4 or later
Summit X650	ExtremeXOS 12.2 or later
ReachNXT	ExtremeXOS 11.2 on the connected switch
	ExtremeXOS 12.2 on the connected switch required for ReachNXT firmware upgrade capability
BlackDiamond 6800	6.2 or later
BlackDiamond 8800	ExtremeXOS 11.1 or later
	ExtremeXOS 12.0 or later for 10G4Ca Module
	ExtremeXOS 12.3 or later for 8900-MSM128, 8900-10G24X-c, and 8900-G96T-c modules
	ExtremeXOS 12.4 or later for 8900-10G8X-xl, 8900-G48X-xl, 8900-G48T-xl, G24Xe, G48T-ep, G48T-e, 8500-MSM24, 8500-G48T-e, 8500-G24X-e, and MSM24 modules
BlackDiamond 8900	ExtremeXOS 12.3 or later
	ExtremeXOS 12.4 or later for 8900-10G8X-xl, 8900-G48X-xl, and 8900-G48T-xl modules
BlackDiamond 10808	ExtremeXOS 11.0 or later
BlackDiamond 12802	ExtremeXOS 12.0 or later
BlackDiamond 12804	ExtremeXOS 11.4 or later
BlackDiamond 20804	ExtremeXOS 12.4 or later
BlackDiamond 20808	ExtremeXOS 12.4 or later

If you have a support contract, you can download the latest versions of ExtremeWare or ExtremeXOS from: http://www.extremenetworks.com/go/esupport.htm.

Switch Access Requirements

Ridgeline SA uses both SNMP and Telnet to discover and communicate with the devices on your network. They support both SNMP v1/v2 or SNMP v3.

- SNMP must be enabled on the switch for Ridgeline SA to discover the device, and for Ridgeline SA to manage the switch.
- If you use access profiles to control SNMP, Telnet and SSH access to your switches, you must ensure that the Ridgeline SA host's IP address is permitted in those access profiles.

Ridgeline SA 2.0 Device Support

With a Base 20 license, Ridgeline SA 2.0 supports up to 20 managed devices. If you want to manage more devices, you can obtain additional 50-node and 250-node licenses from Extreme Networks. The following sections list the devices supported by Ridgeline SA 2.0.

Extreme Networks Device Support

Ridgeline SA 2.0 supports the following Extreme Networks devices:

Table 3: Extreme Networks Devices Supported by Ridgeline SA 2.0

Switches/Modules			
Summit switches:			
Summit1*i* /1*i*SX	Summit24e3	Summit 300-24	SummitPx1*
Summit5*i*TX/LX/SX	Summit48*i*/48S*i*	Summit 300-48	Summit WM 100/1000
Summit7*i*TX/SX	Summit 200-24	Summit 400-24t	Summit WM 20
Summit24e2T/2X*	Summit 200-24fx	Summit 400-24p	Summit WM 3400/3600/ 3700
Summit WM 200/ 2000	Summit 200-48	Summit 400-48	
Summit X150 series:			
Summit X150-24t	Summit X150-48t	Summit X150-24p	
Summit X250 series:			
Summit X250-24tDC	Summit X250-24xDC	Summit X250-48tDC	
Summit X250e series:			
Summit X250e-24t	Summit X250e-24p	Summit X250e-48t	Summit X250e-48p
Summit X250e-24x			
Summit X350 series:			
Summit X350-24t	Summit X350-48t		
Summit X450 series:			
Summit X450-24t	Summit X450a-24t	Summit X450a-24t-DC	Summit X450a-24x
Summit X450-24x	Summit X450a-48t	Summit X450e-24p	Summit X450a-24x-DC
Summit X450e-48p	Summit X450a-48tDC		

Table 3: Extreme Networks Devices Supported by Ridgeline SA 2.0 (continued)

Switches/Modules			
Summit X480 series:			
Summit X480-24x	Summit X480-24x-SS	Summit X480-24x-SS128	Summit X480-24x-10G4X
Summit X480-48t	Summit X480-48t-SS	Summit X480-48t-SS128	Summit X480-48t-10G4X
Summit X480-48x	Summit X480-48x-SS	Summit X480-48x-SS128	Summit X480-48x-10G4X

* Ridgeline SA 2.0 provides only limited support for the Summit24e2, SummitPx1, Summit WM 100/1000, Summit WM 200/2000, and Summit WM 3600/3700. These devices are supported with the same limitations as non-Extreme devices.

Avaya Device Support

Ridgeline SA 2.0 supports the Avaya Integrated Management software version 3.1 and the following Avaya devices:

Table 4: Avaya Devices Supported by Ridgeline SA 2.0

Device	Device	Device
S8300 Media Server	Cajun C360-PWR	4602 IP Phone
S8500B Media Server	Cajun P333T-PWR	4610 IP Phone
S87XX Media Server	Cajun P332G-ML	4620 IP Phone
G250 Media Gateway	Cajun P332GT-ML	4621 IP Phone
G250-BRI Media Gateway		4622 IP Phone
G700 Media Gateway		4624 IP Phone
G350 Media Gateway		4630 IP Phone

Other Third-Party Device Support

Under normal circumstances, Ridgeline SA 2.0 provides limited support for non-Extreme devices that run MIB-II compatible agents. These devices are supported in Inventory and Alarm Manager (for standard SNMP traps).

Ridgeline SA's third-party framework enables the integration of additional devices independently of Ridgeline SA software releases. Over time, this will allow support for selected third-party devices to be added, as well as simplifying the support of new Extreme Networks devices that may be released between Ridgeline SA software releases.

NOTE

Third-party device limitations also apply to the Extreme Summit24e2, the SummitPx1, the Summit WM 100/1000, Summit WM 200/2000, and Summit WM 3600/3700 devices, as well as the Sentriant AG and Sentriant NG devices.

Table 5 provides a summary of Ridgeline SA's basic support for non-Extreme devices.

Table 5: Third-Party Device Support by Feature

Feature	Third-Party Device Support
Inventory	MIB-2 compatible devices: status only, SNMP v1 only. Integrated support for devices included through the Integration Framework.
Alarms	MIB-2 compatible devices: standard traps. Integrated alarm support for devices included through the Integration Framework.
Configuration Manager	No
Firmware Manager	No
IP/MAC Address Finder	No
Telnet	Telnet supported for selected third-party devices. No SSH support.
Real-Time Statistics	No
Map Views	Yes, limited to display on map.
Reports	Limited support for MIB-2 compatible devices

SSH Support

Ridgeline SA supports the use of SSH for communication with Extreme Networks devices if the following conditions are met:

- The SSH Enabling Module must be installed on the Ridgeline SA server host. Due to export restrictions, you must obtain this module from Extreme Networks. It is not included with the Ridgeline SA software distribution.
- Your switches must be running versions of ExtremeWare or ExtremeXOS that support SSH, and SSH must be enabled on those devices. Due to export restrictions, a special license is required for the SSH versions of the switch software. To request SSH-enabled versions of the software, contact Extreme Networks Technical Support.

More information about obtaining and installing these modules can be found in the Ridgeline SA Installation and Upgrade Guide. SSH is not supported for third-party devices.

Ridgeline SA Software Licensing

To log in to the Ridgeline SA Server from a Ridgeline SA Client, Ridgeline SA must be configured with a valid license. You can install the software without a license key, but you cannot connect to it from a Ridgeline SA Client.

- An evaluation license allows you to run the product on a temporary basis and manage a network of up to 2000 nodes. If you want to continue using the product beyond the evaluation period, you must obtain a permanent license.
- A permanent license has no time limit. Permanent licenses are sold based on the number of devices to be managed by the Ridgeline SA system. When you purchase Ridgeline SA, you receive a Base 20 node license, which allows you to manage up to 20 devices. If you want to manage more devices, you can obtain additional 50-node and 250-node licenses from Extreme Networks.

- The Advanced Services Pack license adds VPLS and PBB features to Ridgeline SA.

Both permanent and evaluation license keys are 14-character keys that start with EP and are followed by 12 additional upper- and lower-case alphabetic characters, numbers, and special characters such as "+".

If you have purchased the product, you should have received an activation key, found on the License Agreement that accompanies your software package. This key starts with "AC," and can be used to obtain a permanent license key. You do not need an activation key to obtain an evaluation license key. See "Obtaining a License" on page 20 for more information.

Software Installation or Upgrade Overview

The Ridgeline Service Advisor Installation and Upgrade Guide contains complete instructions for installing the Ridgeline SA Management Suite under Windows, Linux, and Solaris.

The Ridgeline Service Advisor *Installation and Upgrade Guide* can be found in PDF format on the Ridgeline Service Advisor product CD, on the Extreme Networks Ridgeline Service Advisor download web site, or on the Extreme Networks documentation page.

Obtaining a License

Ridgeline Service Advisor requires a valid permanent or evaluation license to be installed before you can log into the Ridgeline SA Server through an Ridgeline SA client. To obtain a license key, use your browser to connect to the license page at http://www.extremenetworks.com/go/ridgeline.htm.

To obtain an evaluation license, select the option to obtain an evaluation license key. You will be asked to enter your name, company information, and other similar information, and an e-mail address to which your license key should be sent. Your license key will be sent to you by return e-mail.

To obtain a permanent license, select the option to obtain a permanent license key. Fill in the requested information, and enter your activation key. The activation key is a 14-character key that starts with "AC" and is found on the License Agreement included with your software package.

Your permanent license key will be sent to you by return e-mail. See the Ridgeline Service Advisor Installation and Upgrade Guide for instructions on running the License Manager to install your license(s).

Ridgeline SA Software Documentation

The Ridgeline SA software documentation set includes installation instructions, context-sensitive Online Help, two user guides, and this release note.

The Ridgeline Service Advisor *Installation and Upgrade Guide* contains documentation on how to install the Ridgeline SA software, or upgrade from a previous version. This is available in PDF format on the Ridgeline SA product CD, in the **extreme.war\helptext\docs** subdirectory of the Ridgeline SA installation, and on Extreme Networks documentation web site. It is also shipped in hardcopy with the Ridgeline SA version 2.0 software package.

The *Ridgeline SA Concepts and Solutions Guide* provides discussions and examples of how to use Ridgeline SA to manage your Extreme Networks installation. It is available in Acrobat PDF format, accessed from the **Programs > Extreme Networks > Ridgeline Service Advisor 2.0** submenu on the Windows **Start** menu. It can also be found in the **extreme.war\helptext\docs** subdirectory of the Ridgeline SA installation.

The *Ridgeline Service Advisor Reference Guide* contains basic documentation on how to use the features of the Ridgeline SA software. Its content forms the basis of the context-sensitive online Help. The Reference Guide is available in Acrobat PDF format, accessed from a link on the Ridgeline SA Welcome page. It can also be found in the **extreme.war\helptext\docs** subdirectory of the Ridgeline SA installation.

For the latest versions of the technical documentation, go to the Extreme Networks web site at:

http://www.extremenetworks.com/services/software-userguide.aspx

2 Clarifications, Known Behaviors, and Resolved Issues

This section describes known problems with the Ridgeline SA 2.0 release, including recommendations for workarounds when available. It also lists problems that existed in previous versions of Ridgeline SA that have been fixed in this release.

Numbers in parentheses are for internal tracking. For the latest release notes, patches, and bug list, see: http://www.extremenetworks.com/go/esupport.htm.

Troubleshooting

If you are having problems with the Ridgeline SA server or client, there are several ways you can capture information that will be helpful to Extreme Networks Technical Support staff.

The Package Ridgeline SA Info command

On the Ridgeline SA server, you can use the **Package Ridgeline SA Info** tool to create a zip format file of all the Ridgeline SA logs, syslog files, property files and other information, which can be sent to your Extreme Networks Technical Support representative for analysis. You can run this tool whether or not the Ridgeline SA server is running.

Client Information from the About window

From a Ridgeline SA client you can display a great deal of status information from the About information window: from the Ridgeline SA **Help** menu, click **About Ridgeline SA**. Information is displayed in a text window; you can cut and paste the information into a file and send it to your Extreme Networks Technical Support representative for analysis.

ExtremeXOS 12.4.2 Dependencies

The following known problems and clarifications require ExtremeXOS 12.4.2 software:

1 **Port Management:** On the Summit X650 switch, 1 Gbps ports are shown as 10 Gbps ports. (PD4-1324391741)

2 **Ridgeline SA Inventory:** When creating VPLS instances, the service VLAN name is not shown. SmartTraps are received, but Ridgeline SA is unable to collect the VLAN data. (PD4-1253879412)

3 **EAPS Provisioning:** Segment health check intervals and common path timers cannot be modified when provisioning EAPS. (PD4-1212941471)

4 **VLAN Configuration:** Paging does not work for CustomerVlanConfig and BVlanConfig. (PD4-1207376781)

Clarifications and Known Problems

The following known problems and clarifications apply to this release:

1 **Inventory:** Single VLAN data collection does not occur for devices with version ExtremeXOS 12.4.1.5 or 12.4.1.9. When VLANs are created or modified on a device and SmarTraps are sent to Ridgeline SARidgeline. Ridgeline SA then polls the device for the new/modified VLAN related configuration changes and updates the new/modified VLAN data. This feature is not working correctly in ExtremeXOS 12.4.1.9. This PD is fixed in ExtremeXOS 12.4.2. (PD4-1195960726)

2 **VPLS:** On multiple next hop (MLT) condition LSPs in use does not show complete path. (PD4-1249312381)

3 **Network Name Modification:** When a network name for a BVLAN/VMAN/VLAN that is associated to a service is changed, the null pointer exception dialog keeps popping up.

Workaround: Associate the network name to the BVLAN/VMAN/VLAN before using it as a transport type to create the service. (PD4-1274233683)

4 **VPLS:** Pseudowire overlay does not highlight LSP in use path if LDP only is configured and enabled on a switch. Engress/ingress interface information is also not shown properly in the table. (PD4-1212815358)

5 **VPLS Status:** VPLS instance status changes on a device will not be reflected in RSA automatically unless manual update or detailed poll. (PD4-1137649903)

6 **VPLS:** VPLS running on a user defined VR is not shown in Ridgeline SA. (PD4-1145478940)

7 **Inventory:** Ridgeline SA shows duplicate device groups and devices when creating a device group and then adding devices. (PD3-26934109, PD3-24802423)

8 **Inventory:** A Summit X250e is showing the wrong port type. (PD4-1373762760)

9 **Port Management:** The Ready port status is not correct between a SummitX250-24t and a SummitX450-t series switch. (PD4-1376515998)

10 **Migration and Upgrade:** After migration, Managed Profiles do not display the default profiles in the Network Profile screen. (PD4-1354666329)

11 **Map Views**: Right clicking on the topology map shows a “Save as” but no “Save" selection. (PD4-1277929658)

12 **Default Selection Box:** The Default selection box is not large enough to read an entire IP address, causing users to resize each box individually. (PD4-1277929593)

13 **Default VLAN:** Ports that are added as untagged ports are only removed from the default VLAN. (PD4-1340961133)

14 **Supported Links:** Selecting a link/device that is not supported for a particular operation, such as Create vMAN or Create BVLAN, results in all the devices/links being listed regardless of the selection. (PD4-1324642896)

15 **Service Overlay:** Even after deleting a service, the service overlay/reading pane still retains all the information about the service. Performing a refresh does not correct this issue. (PD4-1229162531)

16 **Ridgeline SA Client:** If Ridgeline SA Client is launched with a remote desktop connection, the saved SVG map file size is zero. (PD4-1312275071)

17 **SNMP:** Single VLAN data collection fails following an SNMP session related error:

```
SNMP get failed. Error Sending PDU. The Session has not been established.
```

A detail poll also generates SNMP session related messages. (PD4-1070888531)

18 **Reports:** The VLAN Name column is empty in the Unused Ports Report. (PD4-1207225252)

19 **Inventory:** The current Inventory Device view panel contains the following text: To change, click the **Modify** button above." There is no **Modify** button in this window. (PD4-1279910678)

20 **EAPS Control VLAN:** An EAPS control VLAN does not have to be assigned a QP8 by Ridgeline EAPS provisioning. (PD4-1364407944)

21 **VPLS Status:** VPLS status (admin, operational) is shown as Up for VPLS instances that are in a signal state on a device. (PD4-1360898185)

22 **vMAN Provisioning:** vMAN provisioning should validate whether the same ethertype is used in all the switches that are being provisioned. (PD4-1355838218)

23 **PBB Table:** After creating a PBB E-Line/ELAN service, ISID is not shown in the table. Also, the BVLAN network name is not associated with a CVLAN/SVLAN.

Workaround: Manually update the devices associated to the E-Line/E-LAN service. (PD4-1255883070)

24 **Modifying Services:** Modifying a service (adding a port) on the same device should not give an option for customizing settings for CVLANs and SVLANs. (PD4-1296419458)

25 **Map Views:** When a link goes down, its change in status is not updated until a sync is performed. (PD4-1265441595)

26 **EAPS Monitoring:** The Links information in the EAPS domain details window does not include "Load sharing" and "Last updated from database" fields. (PD4-1255709135)

27 **Reports:** When the Reports application was invoked from the Ridgeline SA Client, and opened in a Firefox browser, the "Close Window" link on the Reports page did not actually close the window. (PD4-1274429023)

28 **Inventory:** A port with a speed of 1G was incorrectly reported in Ridgeline SA displays with a speed of 10G (PD4-1276931391)

29 **Inventory:** When using the "Upload Device Information For Support" function, if you selected the "Include extended troubleshooting information", the upload attempt failed after 30 minutes. (PD4-1150255054)

30 **Inventory:** The device panel view for the BlackDiamond 12802 showed a maximum of three power supplies, where up to four power supplies are supported. (PD4-1279548275)

31 **VLAN Details:** If you changed the name of a device, the VLAN details window showed the device's VLANs as associated with the previous name of the device. (PD4-1271685939)

32 **VLAN Provisioning:** After a VLAN was added to a device running ExtremeWare using the VLAN Provisioning feature, the new VLAN did not appear in Ridgeline SA tables. (PD4-1274731674)

33 **Ethernet Service Provisioning:** When adding a port to an Ethernet service that used PBB as the transport method, Ridgeline SA incorrectly presented an option to enter CVLAN and SVLAN information. (PD4-1296419458)

34 **VPLS Monitoring:** When Ridgeline SA encountered a high number of pseudo wire status change traps, it did not process them beyond the default of 20 (default) or 60 (maximum), causing the VPLS domain status to be updated incorrectly. (PD4-1278358796)

35 **Configuration Manager:** Resetting the selection with the **Reset** button, then selecting a device and clicking **Add** caused the first device in the device table to be added instead of the selected device. (PD4-1310142461)

Installing or Uninstalling

Cannot re-install Ridgeline SA after an unsuccessful uninstall

If problems occur during the uninstall process, or if an uninstall is done incorrectly (for example, by just deleting all the Ridgeline SA files) the installation program may refuse to let you re-install because it

still detects the previous installation. To solve this problem the InstallShield Vital Product Data (VPD) registry may need to be cleaned up. This registry is a directory that resides at \Program Files\Common Files\InstallShield\Universal (in Windows) or in ~/InstallShield in Linux or Solaris. You need to remove the directory extremenetworks\epicenter under this VPD registry. Note that other applications may use the InstallShield VPD to store their uninstallation data, so use caution when cleaning the VPD registry. Call your Extreme Networks technical support representative if you need further help. Besides doing what is listed above, for Solaris/Linux platform, do the following:

1 Remove profile file (for both Linux and Solaris)

```
/etc/ridgeline20.profile
```

2 Remove daemons file (for both platforms):

```
/etc/init.d/RidgelineServer20
/etc/init.d/RidgelineDB20
```

3 Remove soft links in Linux:

```
/etc/rc5.d/S74RidgelineDB20
/etc/rc5.d/S75RidgelineServer20
/etc/rc2.d/K10RidgelineServer20
/etc/rc2.d/K11RidgelineDB20
```

4 Remove soft links in Solaris:

```
/etc/rc3.d/S74RidgelineDB20
/etc/rc3.d/S75RidgelineServer20
/etc/rc2.d/K10RidgelineServer20
```

Installing Ridgeline SA on a system with non-English-language character sets

If you are installing Ridgeline SA on a system with non-English-language character sets, make sure the folder names in the directory path where you install Ridgeline SA do not contain any non-English characters. If there are non-English characters in the directory path where Ridgeline SA is to be installed, the installation may fail.

General—Client

Auto-save is on by default when the Ridgeline SA server starts up

When the Ridgeline SA server starts up it syncs all devices, and the auto-save feature is enabled by default. To avoid having auto-save function on your devices, you can disable it through the server properties in Ridgeline SA Administration. If you do not want auto-save to take effect at all, you should disable it before you add your devices to Ridgeline SA. You can do this through the server properties in Ridgeline SA Administration. (PD2-204103816)

Message about Ridgeline SA's digital signature appears twice

When logging in to the Ridgeline SA server, a dialog box indicating that the Ridgeline SA application's digital signature could not be verified may appear twice. (PD3-139718617)

Multibyte-encoded characters display incorrectly in Ridgeline SA Client

If you create a device group that includes multibyte-encoded characters (such as Japanese characters) in its name, the device group name may not display correctly in Ridgeline SA. The Ridgeline SA Client does not support character sets that use multibyte encoding. (PD4-314415318)

Connection error when Ridgeline SA server and client are in different domains

When the Ridgeline SA server and client were in different domains, the client was unable to connect to the server even though the server was reachable using its fully qualified domain name. As a workaround, you can edit the `/etc/ridgeline20.profile` file and change the `EPICENTER_SERVER_ADDRESS` value to the IP address of the server. (PD4-992968741)

General—Server

TFTP port remains in use after Ridgeline SA TFTP server disabled

After disabling the Ridgeline SA TFTP server, the TFTP port remains in use. Restart the system to clear it. (PD3-24495867)

Traps may be dropped if the trap rate becomes excessive

In order to be able to reliably handle trap storms from a single or multiple devices, Ridgeline SA limits its trap processing to 20 traps every 28 seconds from an individual device, and a total of 275 traps every 55 seconds system-wide. Any traps that occur beyond these limits are discarded, but will be noted in the `log.txt` file. If a sufficiently long burst of traps occurs, some of them may be dropped.

Exceeding the first limit (>20 traps in 28 seconds for a single device) is rare. However, if you are managing a large number of devices, it is possible to exceed the total (275) limit. (PD3-103525231)

Stopping the Ridgeline SA database prior to stopping the server

When stopping the Ridgeline SA server, if you stop the database component prior to stopping the server component, the Java process may still continue. Make sure that you stop the server component prior to stopping the database component. (PD4-436834851)

Network Views

Incorrect display of load-shared links

Ridgeline SA incorrectly displayed a single load-shared link consisting of three links as three separate load-shared links. To work around this, update the two devices on either end of the load-shared link, and then use the **Clear inactive links** function. This will show correct load sharing information. (PD4-484009799)

Error when disabling EAPS primary port if EAPS ring was displayed in the Map View

If the primary port in an EAPS node was disabled while the EAPS ring was displayed in the Ridgeline SA Map View, it resulted in an IllegalArgumentException error. (PD4-707645154)

Updated EAPS information not displayed in the Table View

When the status of an EAPS domain changed, the updated information was displayed in the Map View, but not the Table View. (PD4-709785677)

Invalid Session message displayed when saving a map

If the Ridgeline SA server is experiencing network connectivity problems, such as dropped packets, it may result in an "Invalid Session" message displayed on a remote client attempting to save a map view. (PD4-988967106)

Alarm Manager

HTTP unreachable alarms not generated for certain devices

HTTP unreachable alarms were not generated for devices that had their HTTP services disabled prior to when the HTTP unreachable alarm was configured and enabled. (PD4-699276054)

Incorrect Power Supply Failed alarm generated for SNMP-unreachable devices

Ridgeline SA incorrectly generated a Power Supply Failed alarm when a device was SNMP unreachable. (PD4-788565691)

CPU Utilization threshold comes back after being deleted

In Alarm Manager, if you deleted the CPU Utilization threshold for a device, the next time the device was synchronized, the CPU Utilization threshold for the device was again visible in the Alarm Manager. (PD4-938840527)

Configuration Manager

Downloading a config file to device fails if using SSH

Downloading a configuration file to a device running ExtremeWare may fail if Ridgeline SA attempts to use SSH to the device. If this occurs, to successfully download a configuration through Ridgeline SA, you must temporarily disable SSH for the device. (PD3-102888481)

Changing the Diff or Config file viewer settings does not work properly

Changing the settings for the configuration file viewer or the Diff viewer does not work properly when the client is connected to a Linux server. For the configuration viewer it will attempt to use the viewer configured on the server; for a Diff it uses **sdiff**, which is available locally. (PD3-91990375)

Refreshing the Configuration Manager window after a Schedule Baseline operation

After a Schedule Baseline operation is completed, the information in the Configuration Manager window does not get refreshed, even after clicking the Refresh button. As a workaround, you can restart the Ridgeline SA client application. (PD4-695935840)

Device/Port Grouping

Cannot have identically named Device and Port groups at the same level

In this release, it is not possible to create an identically named port group and device group at the same level in the group hierarchy. (PD4-366149982)

Error when creating a new group while deleting another group

If you deleted a group consisting of many subgroups, attempting to create a new group while the deletion was in progress produced an error message. (PD4-422019493)

Error when moving devices to a large group

When moving devices to a group consisting of a large number of devices (more than 200), Ridgeline SA produced an error message. (PD4-524358195)

Java error when copying a top-level group to another top-level group

Copying a top-level group that includes a subgroup to another top-level group causes a Java runtime exception error. (PD4-697359803)

Stacking devices may not be displayed in the Hardware Selection page

In the Upgrade Wizard, if you select an ExtremeWare or ExtremeXOS stacking image in the Image Selection page, then select “Extreme Stacking” or “Extreme EXOS Stacking” under Device Types on the Supported Hardware Selection page, devices of the selected type are not displayed in the Hardware Selection page.

Inventory Management

Modify Device changed fields are not updated after Apply

When a change is made in the Modify Device dialog, after clicking **Apply** the change is not reflected in the fields in the Modify Device window. You must close and re-open the Modify Device dialog to see the changes. (PD3-89128855)

Additional Information field accepts more than 255 characters

Even though there is a 255-character limit on text in the Additional Information field, you can type more than that into the field. However, the characters beyond 255 will not be saved. (PD3-82612460)

The Upload Device Info command does not work with SSH

The Upload Device Info command, used for uploading device status information, does not work if SSH is enabled for the device in Ridgeline SA, due to a timeout. To successfully upload the device information, you must temporarily disable SSH for the device.

The ExtremeXOS config file saved by the Upload Device Info command has errors

If you use the Upload Device Info command for a device running ExtremeXOS, and select the option to include the last uploaded configuration file, the Configuration file saved within the **TAC_Info** zip file will produce CRC errors when you attempt to unzip it. (PD3-106577660)

BD8810 port containing a 100Base-FX mini-GBIC displayed as a UTP port

Ridgeline SA incorrectly displayed a Black Diamond 8810 port containing a 100Base-FX mini-GBIC as a UTP port. (PD4-983773008)

IP/MAC Address Finder

Ridgeline SA does not use VRs when pinging, resulting in errors on some ExtremeXOS devices

In the IP/MAC Address Finder, Ridgeline SA pings without using any VR, thus using VR-default only. If some ExtremeXOS switches are in VR-mgmt, this results in a packet transmit error. (PD3-90286092)

Real-Time Statistics

Hierarchical port groups are not displayed correctly in the RT Statistics applet

The Real-Time Statistics applet does not support hierarchical groups. Selecting a subgroup of a port group is not recognized; selecting the top-level port group initially displays all ports in the group and

its subgroups at the same level, then changes the display to show only the ports in the top level group. (PD3-40487688)

Reports

User Defined Reports link does not appear the first time Reports are invoked

When you display the Reports feature for the first time after installing Ridgeline SA 2.0, the User Defined Reports link does not appear. Once you refresh the browser, the link appears and works properly from then on. (PD3-106204511).

Internal power supplies reported as failed rather than powered off on Summit X250 or X450 devices

For Summit X250 or X450 devices with external power supplies connected, the "Devices in Marginal Condition" report incorrectly showed the internal power supplies for these devices as failed power supplies, instead of powered off. (PD4-700644264)

Telnet

Cannot edit ExtremeXOS Policy files in the Telnet window

The Ridgeline SA Telnet window does not support the editing of ExtremeXOS policy files. (PD3-55109713)

VLAN Management

Cannot create a VLAN Network Name with the same name as a device/port group

It was not possible to create a VLAN Network Name that had the same name as an existing device or port group, nor was it possible to create a device or port group with the same name as an existing VLAN Network Name. (PD4-487584301)

Enabling "Show VLANs" in the Link Details window displayed incorrect information

In the Link Details window, enabling the Show VLANs box did not display correct VLAN information. The VLAN information is displayed correctly in the VLAN tab. (PD4-699276059)

Avaya-Ridgeline SA Integration

NOTE

These items apply only to customers with the Avaya Integrated Management server version 3.1 co-resident with the Ridgeline SA server.

Ridgeline SA complains about missing device when launched from AIM

When Ridgeline SA is launched from the Avaya Integrated Management software, it complains that "Device 127.0.0.1" is not in Inventory. You can ignore this message. (PD3-102012039)

Attempting to launch Ridgeline SA from the browser-based AIM Console fails

If you launch the AIM console in a browser window, and then attempt to launch Ridgeline SA, the Ridgeline SA browser window never opens. This does not happen consistently, and is most likely to happen when the browser client is running on the same system as the Ridgeline SA and AIM servers. (PD3-102011941)

Profile Manager

Ridgeline SA does not enforce the maximum number of profiles

The Universal Port feature allows a maximum of 128 profiles on an Extreme device. However, in the current release, Ridgeline SA does not enforce this maximum number. Ridgeline SA allows you to deploy more than 128 profiles to a switch, but the configuration fails. (PD3-133538459)

Profiles bound to USER-REQUEST events are executed at the time of deployment

If you bind a profile to a USER-REQUEST event, the profile is executed at the time of deployment, even if the profile is disabled in Ridgeline SA.

Scripting

Error when trying to save a Ridgeline SA script

After logging into the Ridgeline SA server using RADIUS authentication, if you created and saved a Ridgeline SA script, then edited the script and attempted to save it again, Ridgeline SA displayed a message indicating that the script could not be saved. As a workaround, you can select the **Save As** option and overwrite the existing script. (PD4-984769971)